## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. A method for communicating cryptographic data through multiple network layers, comprising:

receiving the cryptographic data at a node;

dividing the cryptographic data into multiple pieces; and

encapsulating different pieces of the cryptographic data in fields associated with different network layers of a protocol stack in a data packet, ~~whereby~~ wherein the cryptographic data ~~that~~ is ~~too~~ larger than ~~to be communicated in~~ a single field ~~can be~~, and wherein the cryptographic data is encapsulated within~~communicated through~~ multiple fields associated with different network layers of the protocol stack.

2. The method of claim 1, wherein receiving the cryptographic data involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.

3. The method of claim 2, wherein the input data includes a public key associated with the node.

4. The method of claim 2, wherein the input data includes a static identifier associated with the node.

5. The method of claim 2, wherein an IPv6 address field of the data packet is comprised of a 64-bit prefix followed by the most-significant 64 bits of

the output of the non-reversible function, and wherein a universal/local bit and an individual/group bit of the IPv6 address are both set to “0”.

6. The method of claim 5, wherein a SIP Call-ID field of the data packet is comprised of a local-id and a host address, wherein

the local-id is comprised of the least-significant 128 bits of the output of the non-reversible function; and wherein

the host address is comprised of the IPv6 address.

7. The method of claim 2, wherein an SSH public-key fingerprint field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

8. The method of claim 2, wherein a MAC address field of the data packet is comprised of the least-significant 64 bits of the output of the non-reversible function.

9. The method of claim 2, wherein a JXTA Peer-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

10. The method of claim 2, wherein a JXTA Group-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

11. An apparatus for communicating cryptographic data through multiple network layers, comprising:

a receiving mechanism configured to receive the cryptographic data at a node;

a dividing mechanism configured to divide the cryptographic data into multiple pieces; and

an encapsulation mechanism configured to encapsulate different pieces of the cryptographic data in fields associated with different network layers of a protocol stack in a data packet, ~~whereby~~ wherein the cryptographic data ~~that~~ is ~~too~~ larger than ~~to be communicated in~~ a single field, and wherein the cryptographic data ~~can be communicated through~~ is encapsulated within multiple fields associated with different network layers of the protocol stack.

12. The apparatus of claim 11, wherein the receiving mechanism is configured to perform at least one non-reversible function on a piece of input data to produce the cryptographic data.

13. The apparatus of claim 12, wherein the input data includes a public key associated with the node.

14. The apparatus of claim 12, wherein the input data includes a static identifier associated with the node.

15. The apparatus of claim 12, wherein an IPv6 address field of the data packet is comprised of a 64-bit prefix followed by the most-significant 64 bits of the output of the non-reversible function, and wherein a universal/local bit and an individual/group bit of the IPv6 address are both set to "0".

16. The apparatus of claim 15, wherein a SIP Call-ID field of the data packet is comprised of a local-id and a host address, wherein

the local-id is comprised of the least-significant 128 bits of the output of the non-reversible function; and wherein

the host address is comprised of the IPv6 address.

17. The apparatus of claim 12, wherein an SSH public-key fingerprint field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

18. The apparatus of claim 12, wherein a MAC address field of the data packet is comprised of the least-significant 64 bits of the output of the non-reversible function.

19. The apparatus of claim 12, wherein a JXTA Peer-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

20. The apparatus of claim 12, wherein a JXTA Group-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

21. A computer system for communicating cryptographic data through multiple network layers, comprising:

a central processing unit;

a semiconductor memory;

a receiving mechanism configured to receive the cryptographic data at a node;

a dividing mechanism configured to divide the cryptographic data into multiple pieces; and

an encapsulation mechanism configured to encapsulate different pieces of the cryptographic data in fields associated with different network layers of a protocol stack in a data packet,~~;~~

~~whereby~~ wherein the cryptographic data ~~that~~ is ~~too~~ larger than ~~to be communicated in~~ a single field, and wherein the cryptographic data ~~can be~~

~~communicated through~~ is encapsulated within multiple fields associated with different network layers of the protocol stack.

22. The computer system of claim 21, wherein the receiving mechanism is configured to perform at least one non-reversible function on a piece of input data to produce the cryptographic data.

23. The computer system of claim 22, wherein the input data includes a public key associated with the node.

24. The computer system of claim 22, wherein the input data includes a static identifier associated with the node.

25. The computer system of claim 22, wherein an IPv6 address field of the data packet is comprised of a 64-bit prefix followed by the most-significant 64 bits of the output of the non-reversible function, and wherein a universal/local bit and an individual/group bit of the IPv6 address are both set to “0”.

26. The computer system of claim 25, wherein a SIP Call-ID field of the data packet is comprised of a local-id and a host address, wherein

the local-id is comprised of the least-significant 128 bits of the output of the non-reversible function; and wherein

the host address is comprised of the IPv6 address.

27. The computer system of claim 22, wherein an SSH public-key fingerprint field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

28. The computer system of claim 22, wherein a MAC address field of the data packet is comprised of the least-significant 64 bits of the output of the non-reversible function.

29. The computer system of claim 22, wherein a JXTA Peer-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

30. The computer system of claim 22, wherein a JXTA Group-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

31. A method for verifying a data packet containing cryptographic data, comprising:

receiving the data packet;

extracting pieces of cryptographic data from fields associated with different network layers of a protocol stack within the data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is encapsulated within multiple fields; and

verifying that each piece of extracted cryptographic data matches with a corresponding portion of a piece of previously obtained cryptographic data.

32. The method of claim 31, wherein the previously obtained cryptographic data is obtained through a process that involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.

33. An apparatus for verifying a data packet containing cryptographic data, comprising:

a receiving mechanism configured to receive the data packet;

an extracting mechanism configured to extract pieces of cryptographic data from fields associated with different network layers of a protocol stack

within the data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is encapsulated within multiple fields; and

a verification mechanism configured to verify that each piece of extracted cryptographic data matches with a corresponding portion of a piece of previously obtained cryptographic data.

34. The apparatus of claim 33, wherein the previously obtained cryptographic data is obtained through a process that involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.

35. A computer system for verifying a data packet containing cryptographic data, comprising:

a central processing unit;

a semiconductor memory;

a receiving mechanism configured to receive the data packet;

an extracting mechanism configured to extract pieces of cryptographic data from fields associated with different network layers of a protocol stack within the data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is encapsulated within multiple fields; and

a verification mechanism configured to confirm that each piece of extracted cryptographic data matches with a corresponding portion of a piece of previously obtained cryptographic data.

36. The computer system of claim 35, wherein the previously obtained cryptographic data is obtained through a process that involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.